

**Notice of Allowability**

Application No.

10/623,830

Examiner

Chat C. Do

Applicant(s)

ELBE ET AL.

Art Unit

2124

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 09/29/04.
2. ☒ The allowed claim(s) is/are 1-13.
3. ☒ The drawings filed on 21 July 2003 are accepted by the Examiner.
4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☒ All b) ☐ Some\* c) ☐ None of the:
    1. ☒ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |   |   |
|---|---|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892)  | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)           |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                | 6. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date _____ |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),<br>Paper No./Mail Date _____ | 7. <input type="checkbox"/> Examiner's Amendment/Comment                              |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material          | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance  |
|   | 9. <input type="checkbox"/> Other _____   |

### REASONS FOR ALLOWANCE

1. Claims 1-13 are allowed.
2. The following is an examiner's statement of reasons for allowance:

The prior art of records fails to disclose or render obviousness a method for modular multiplying a polynomial multiplicand by a polynomial multiplier within a cryptographic calculation comprising: a multiplication look-ahead step to obtain a multiplication shift value; multiplying variable raised to the power of multiplication shift value by an intermediate result polynomial; performing a reduction look-ahead method to obtain a reduction shift value wherein reduction shift value being equal to the difference of the degree of shifted intermediate result polynomial and the degree of modulus polynomial; multiplying variable raised to the power of reduction shift value; and summing shifted intermediate result polynomial and subtracting shifted modulus polynomial to obtain an updated intermediate result as cited in independent claims 1 and

7.

The closest found prior art is Sedlak (U.S. 4,870,681). Sedlak discloses a method for modular multiplying a multiplicand by a polynomial multiplier within a cryptographic calculation comprising: a multiplication look-ahead step to obtain a multiplication shift value; multiplying variable raised to the power of multiplication shift value by an intermediate result; performing a reduction look-ahead method to obtain a reduction shift value; multiplying variable raised to the power of reduction shift value; and summing

Art Unit: 2124

shifted intermediate result polynomial and subtracting shifted modulus to obtain an updated intermediate result. However, Sedlak fails to disclose the operands, multiplicand, multiplier, and modulo being polynomials of a variable and the reduction shift value being equal to the difference of the degree of shifted intermediate result polynomial and the degree of modulus polynomial as seen above.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chat C. Do whose telephone number is (571) 272-3721. The examiner can normally be reached on M => F from 7:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chaki Kakali can be reached on (571) 272-3719. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Application/Control Number: 10/623,830

Page 4

Art Unit: 2124

Chat C. Do  
Examiner  
Art Unit 2124

December 22, 2004

*Kakali Chaki*

KAKALI CHAKI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100